(12) UK Patent Application (19) GB (11) 2 317 983 (13) A

(43) Date of A Publication 08.04.1998

(21) Application No 9721224.5

(22) Date of Filing 06.10.1997

(30) Priority Data
(31) 96044125 (32) 05.10.1996 (33) KR

(51) INT CL[6]
G07F 19/00 , G06F 1/00 , H04L 9/32

(52) UK CL (Edition P)
G4H HTG H13D H14A H14B H14D

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition P) G4H HTG , H4P PDCSA
INT CL[6] G06F , G07F , H04L

(71) Applicant(s)
Samsung Electronics Co Limited

(Incorporated in the Republic of Korea)

416 Maetan-dong, Paldal-gu, Suwon-city, Kyungki-do, Republic of Korea

(72) Inventor(s)
Ju-yeol Yu
Ho-suk Chung
Soon-il Moon

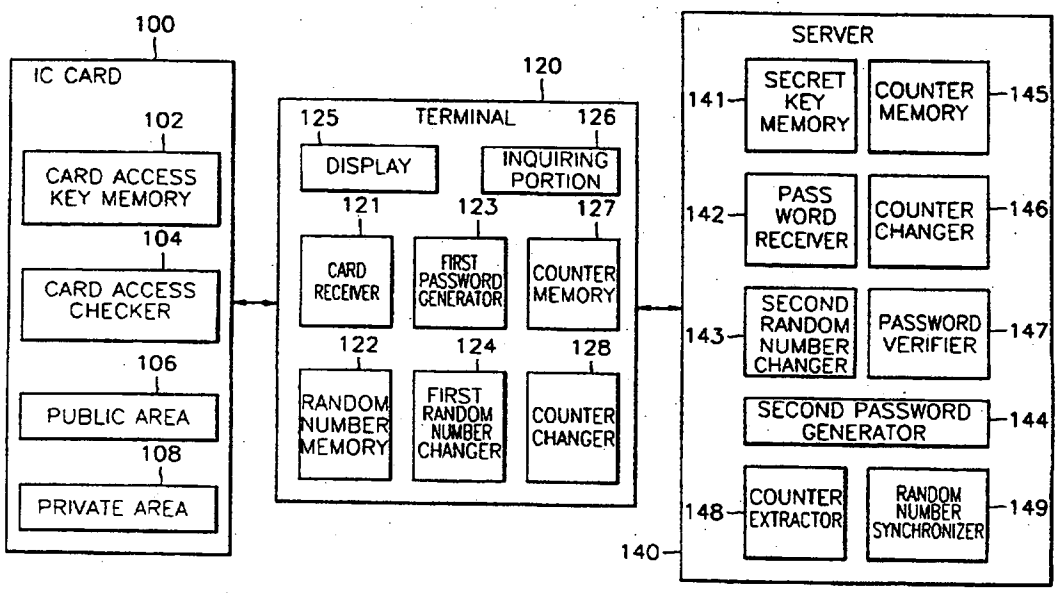
(74) Agent and/or Address for Service
R G C Jenkins & Co
26 Caxton Street, LONDON, SW1H ORJ, United Kingdom

(54) Authenticating user

(57) An apparatus for authenticating a user includes an integrated circuit (IC) card for storing a secret key for generating a one time password and also storing predetermined random numbers. A terminal includes a card receiver for receiving the IC card, a random number memory for reading and storing, and then deleting the random numbers of the IC card, a first password generator for generating a one time password using the secret key of the IC card and one of the random numbers, a first random number changer for changing the random number stored in the random number memory in a predetermined way and storing the changed value, and a display for displaying the password. A server receives the password and compares it with one which it generates from stored values in a similar way, for verification.

It is possible to raise the security level by using a one time password in which a different password is used each time a user is authenticated, and to save costs by generating a one time password for each of various services with a single terminal.

FIG. 1



GB 2 317 983 A

FIG. 1

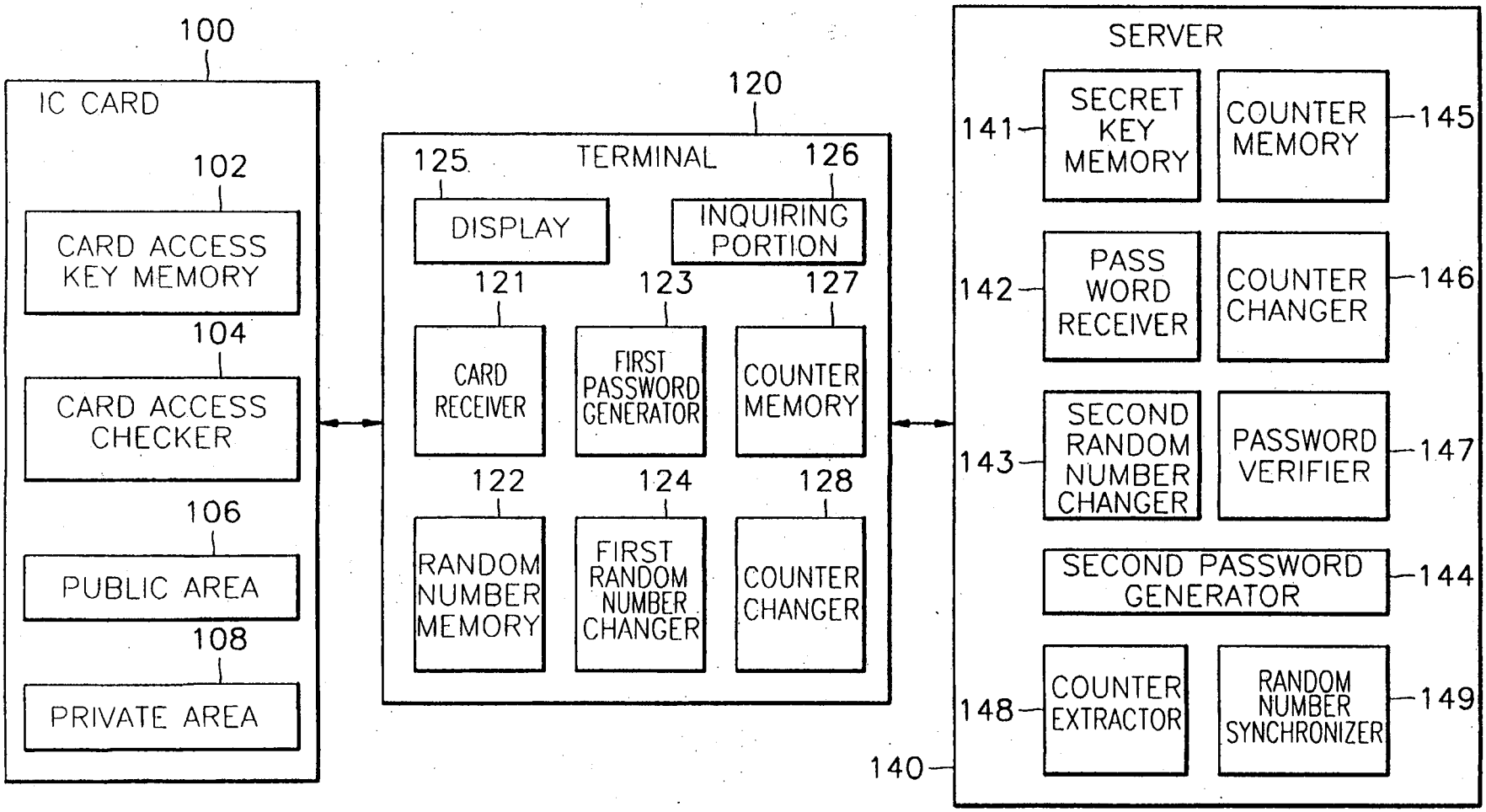

100
IC CARD
102
CARD ACCESS KEY MEMORY
104
CARD ACCESS CHECKER
106
PUBLIC AREA
108
PRIVATE AREA
120
TERMINAL
125
DISPLAY
126
INQUIRING PORTION
121
CARD RECEIVER
123
FIRST PASSWORD GENERATOR
127
COUNTER MEMORY
122
RANDOM NUMBER MEMORY
124
FIRST RANDOM NUMBER CHANGER
128
COUNTER CHANGER
SERVER
141
SECRET KEY MEMORY
145
COUNTER MEMORY
142
PASS WORD RECEIVER
146
COUNTER CHANGER
143
SECOND RANDOM NUMBER CHANGER
147
PASSWORD VERIFIER
144
SECOND PASSWORD GENERATOR
148
COUNTER EXTRACTOR
149
RANDOM NUMBER SYNCHRONIZER
140

FIG. 2

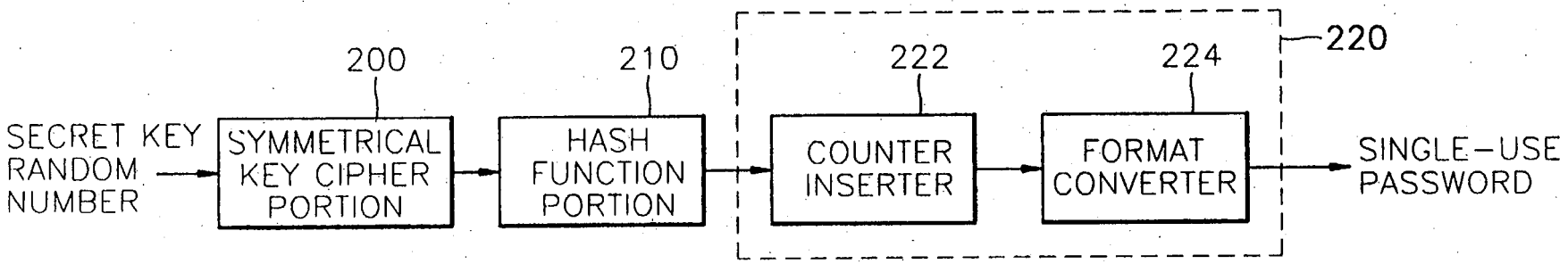

SECRET KEY RANDOM NUMBER
200
SYMMETRICAL KEY CIPHER PORTION
210
HASH FUNCTION PORTION
220
222
COUNTER INSERTER
224
FORMAT CONVERTER
SINGLE-USE PASSWORD

FIG. 3

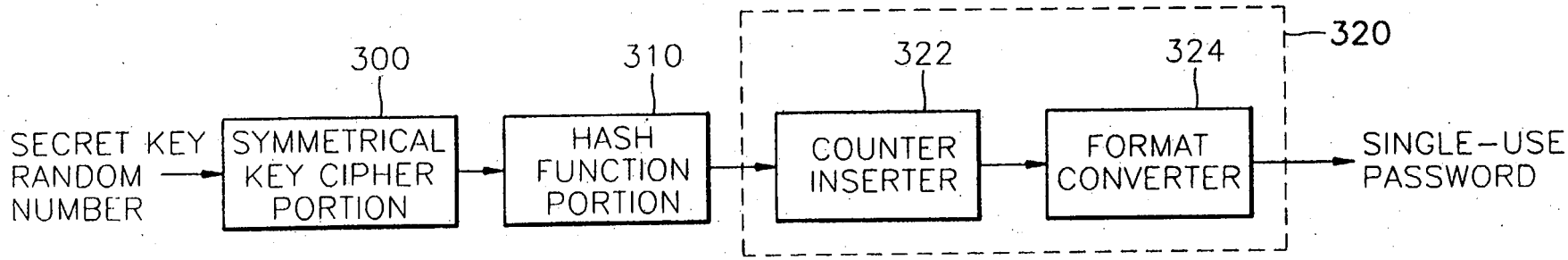

SECRET KEY RANDOM NUMBER
300
SYMMETRICAL KEY CIPHER PORTION
310
HASH FUNCTION PORTION
320
322
COUNTER INSERTER
324
FORMAT CONVERTER
SINGLE-USE PASSWORD

FIG. 4

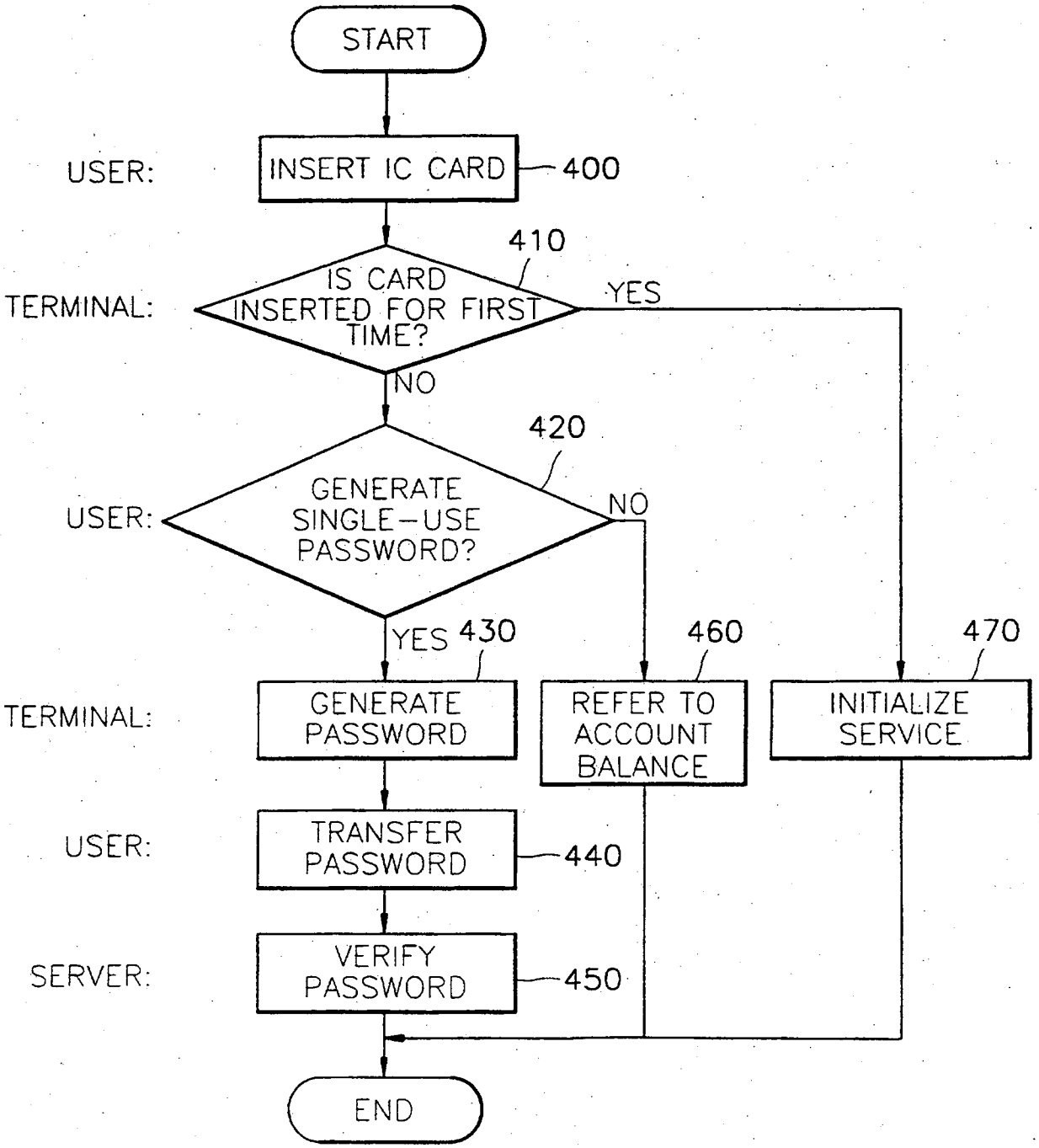

START
USER:
INSERT IC CARD
400
410
TERMINAL:
IS CARD INSERTED FOR FIRST TIME?
YES
NO
420
USER:
GENERATE SINGLE-USE PASSWORD?
NO
YES
430
460
470
TERMINAL:
GENERATE PASSWORD
REFER TO ACCOUNT BALANCE
INITIALIZE SERVICE
USER:
TRANSFER PASSWORD
440
SERVER:
VERIFY PASSWORD
450
END

FIG. 5

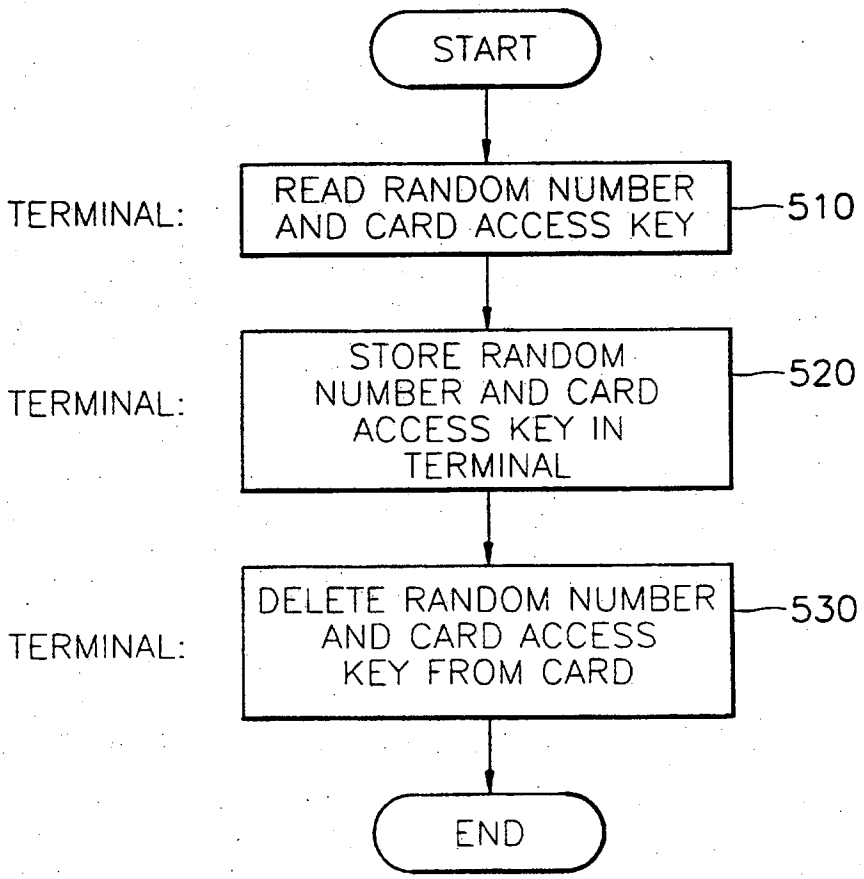

START
TERMINAL:
READ RANDOM NUMBER AND CARD ACCESS KEY
510
TERMINAL:
STORE RANDOM NUMBER AND CARD ACCESS KEY IN TERMINAL
520
TERMINAL:
DELETE RANDOM NUMBER AND CARD ACCESS KEY FROM CARD
530
END

FIG. 6

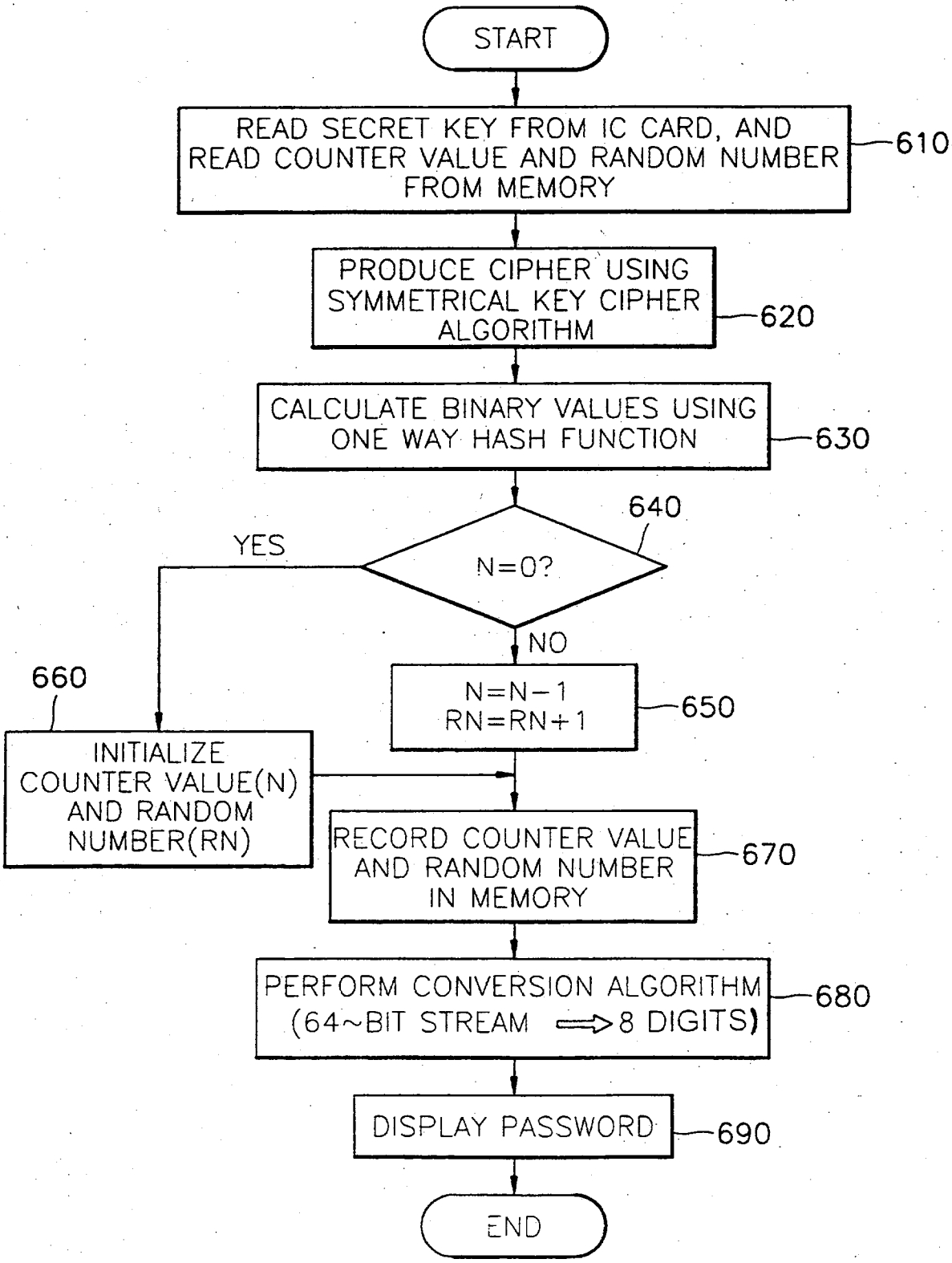
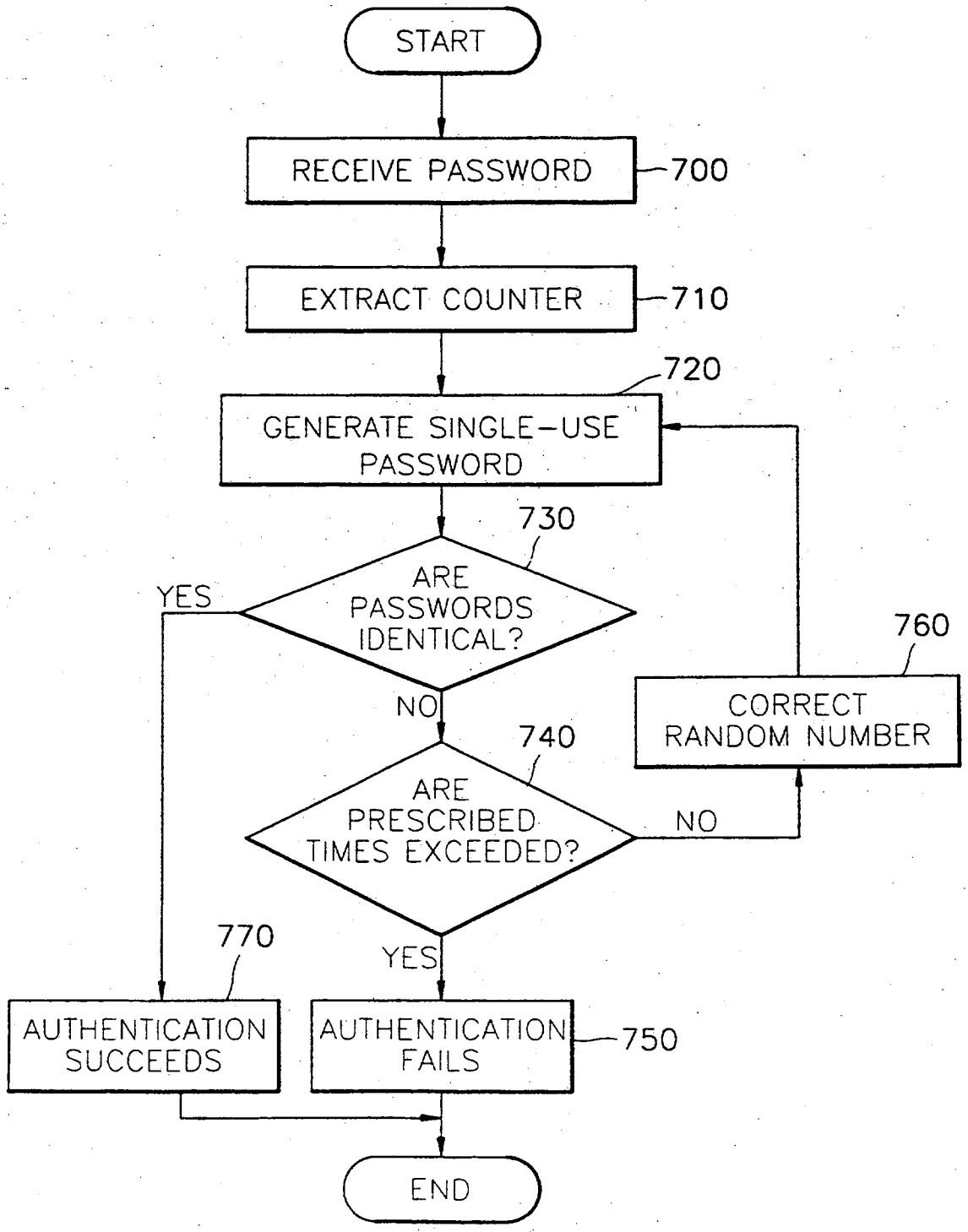

START
READ SECRET KEY FROM IC CARD, AND READ COUNTER VALUE AND RANDOM NUMBER FROM MEMORY
610
PRODUCE CIPHER USING SYMMETRICAL KEY CIPHER ALGORITHM
620
CALCULATE BINARY VALUES USING ONE WAY HASH FUNCTION
630
640
N=0?
YES
NO
660
INITIALIZE COUNTER VALUE(N) AND RANDOM NUMBER(RN)
N=N-1
RN=RN+1
650
RECORD COUNTER VALUE AND RANDOM NUMBER IN MEMORY
670
PERFORM CONVERSION ALGORITHM (64~BIT STREAM ⟹ 8 DIGITS)
680
DISPLAY PASSWORD
690
END

FIG. 7


START
RECEIVE PASSWORD
700
EXTRACT COUNTER
710
720
GENERATE SINGLE-USE PASSWORD
730
ARE PASSWORDS IDENTICAL?
YES
NO
760
CORRECT RANDOM NUMBER
740
ARE PRESCRIBED TIMES EXCEEDED?
NO
YES
770
AUTHENTICATION SUCCEEDS
AUTHENTICATION FAILS
750
END

APPARATUS FOR AUTHENTICATING USER AND METHOD THEREFOR

Background of the Invention

The present invention relates to a user authenticating system, and more particularly, to an apparatus for authenticating a user using a portable terminal and an integrated circuit (IC) card which can refer to an account balance and transaction records of electronic money and can generate a single-use or ephemeral password, and a method therefor.

Various application fields are generated and much convenience is served to people due to the development of computers and communication, the spread of computer networks, and the development of integrated circuit (IC) card technology having memory and computation ability. The electronic money which is one of the applied fields of the IC card should be able to refer to an account balance and transaction records in an electronic purse.

Also, a user can manage money in his or her account without going to a bank, and can easily perform many things by a remote connection using a computer in his or her house. At this time, a service provider such as a bank and a network server must confirm whether a person who wants a service is the authorized user. If an attempt by a person who pretends to be the authorized user succeeds due to a weak user authentication system, invasion of privacy and mental and material damages are caused. In particular, when a

user wants a service from a distance, the service provider needs a method for confirming the user's identity without meeting the user in person.

In order to authenticate the user's identity, what only the user knows, what only the user owns, or physical characteristics or habits unique to the user can be used. The most basic and general method used for authenticating the user's identity is using a password. In a password method, the user's identity is authenticated by confirming what only the user knows. Namely, the user who wants a service selects a password only he or she knows and registers it with the service provider (the server). The user generally uses a string of several numbers or letters as a password. When the user who wishes his or her identity to be authenticated transmits the password to the server, the server compares the transmitted password with the password registered in the inital stage, and authenticates the user.

For a safer user authentication, it is preferable to use a one time password, in which the password is changed each time the user wishes to be authenticated. In this method, an unauthorized access attempter cannot reuse a password he or she found out, since a password is changed each time the user wishes to be authenticated. In order to authenticate the identity using the one time password, an apparatus for generating the one time password is necessary. At this time, if every user uses a terminal of his or her own for generating the one time password, it is possible to improve security, since it is

possible to simultaneously confirm what only the user knows and what only the user owns in order to authenticate the user.

In the one time password, variables which change every time are necessary in order to generate passwords which change every time, unlike in a conventional password. For this, a method of using real time clock (RTC) and a challenge/response method of using random numbers are used.

In the user authentication method in which the RTC is used as a variable, the terminal owned by a user and the server of a service provider are synchronized. Namely, the user is authenticated by comparing the one time password generated according to the time in the terminal, at the time which the user wishes to be authenticated, with the password generated by the server at the same time.

In the challenge/response method of using random numbers, random numbers generated using a random number generator are used in order to determine the one time password. When the user authentication begins, the server generates random numbers and transmits them to the user. The terminal ciphers the random numbers by a secret number shared with the server, generates the one time password, and transmits it to the server. The server authenticates the user by generating a password using the same secret number shared with the terminal and the same random numbers transmitted, and comparing it with the password generated by the terminal.

Meanwhile, the above-mentioned user authentication methods in which the password is used, which are most widely used at present, have many problems. The password generated of several numbers or letters based on personal information such as a telephone number, a birthday, and a resident ID number may be easily found out by others. When the user records the password somewhere, in order not to forget it, it may be exposed to others. In the case that the user who wants a service from a distance delivers his or her password to the server through a telephone line or a network in order to be authenticated, the password may be easily exposed to others by a wiretap.

In the user authentication method in which the RTC is used, the time in the terminal owned by the user is synchronized with the time in the server of the service provider for the generation of the one time password and the user authentication. If the terminal loses synchronization with the server with the lapse of time, then even the authorized user is not authenticated, since the password generated by the terminal does not coincide with the password generated by the server. A special apparatus is necessary in order to synchronize the terminal with the server. Therefore, when the one time password is used in order to strengthen the user authentication in a conventional applied service, a special server is necessary for synchronizing the time in the terminal with the time in the server, thus causing great expense for the service provider. Also, a terminal can generate one time passwords for only one service, since the variables used in the terminal for generating the

password using the real time clock are the real time clocks. When the user wants various applied services, a separate terminal is required for each service.

In the above-mentioned challenge/response method in which random numbers are used, the random numbers transmitted by the server must be input to the terminal in order to generate the one time password. For this, the terminal must include an input device. Also, since a process is necessary in which the server transfers the random numbers to the user and the user inputs the random numbers to the terminal, it takes a long time and is inconvenient for the user. Also, in the case that the server cannot transmit the random numbers to the user, this method cannot be used.

Summary of the Invention

It is an objective of the present invention to provide an apparatus for authenticating a user in which a portable terminal and an IC card, which can refer to an account balance and transaction records of electronic money and can generate a one time password, are used in order to inexpensively and safely authenticate the user.

To achieve the above objective, there is provided an apparatus for authenticating a user, comprising an integrated circuit (IC) card for storing a secret key for generating a one time password and predetermined random numbers, a terminal for generating a one time password using the IC card as

an input, and a server for authenticating the one time password generated by the terminal. The terminal comprises a card receiver for receiving and interfacing with the IC card, and determining whether the IC card is input for the first time, a random number memory for reading and storing, and then deleting the random numbers of the IC card when the IC card is inserted for the first time into the card receiver, a first password generator for generating a one time password by reading the secret key of the IC card and the random number stored in the random number memory, a first random number changer for changing the random number stored in the random number memory into a predetermined value and storing the changed value in the random number memory when a one time password is generated in the first password generator, and a display for displaying the processed results of the terminal and the server. The server comprises a secret key memory for storing a secret key and a predetermined random number identical to the secret key and a predetermined random number initially stored in the IC card, a second password generator for reading the secret key and the random number stored in the secret key memory and for generating a one time password by the same method as used in the terminal, a second random number changer for changing the random number value of the secret key memory into a value identical to the random number changer of the terminal, and storing the changed value in the secret key memory when a one time password is generated by the second password generator, a password receiver for receiving

the one time password generated in the terminal through a telephone line or a network, and a password verifier for verifying whether the received password is identical to the generated password.

The IC card further comprises a card access key memory comprising a public area, to which access is allowed unconditionally, and a private area for which a card access key is required to allow access from the outside for safely storing a card access key required for allowing access to the secret area, and a card access checker for determining whether access to internal information should be allowed, by comparing the card access key input from the outside with the card access key stored in the card access key memory. The random number memory of the terminal reads the random number and card access key of the IC card and stores them, and deletes the random number and card access key from the public area of the IC card, when the IC card is inserted into the card receiver for the first time.

The first password generating portion of the terminal comprises a symmetrical key cipher portion for reading the secret key of the IC card and the random number of the random number memory and generating a cipher using a symmetrical key cipher algorithm, a hash function portion for converting the cipher generated in the symmetrical key cipher portion, using a one way hash function, to prevent an inverse trace of the secret key, and a format converter for converting the cipher output from the hash function portion into a predetermined format. The second password generating portion

of the server comprises a symmetrical key cipher portion for reading the secret key and the random number stored in the secret key storing portion and for generating a cipher using a symmetrical key cipher algorithm, a hash function portion for preventing an inverse trace of the cipher generated in the symmetrical key cipher portion, using a one way hash function, and a format converter for converting the cipher output from the hash function portion into a predetermined format.

To achieve the above objective, there is provided a method for authenticating a user, using a user authenticating apparatus comprising an IC card for storing a predetermined random number and a secret key for generating a one time password, a terminal for generating a one time password using the IC card as an input, and a server for storing the secret key and a random number identical to those of the IC card and for authenticating the one time password generated in the terminal, comprising the steps of inserting the IC card into the terminal, determining whether the IC card is input to the terminal for the first time, initializing a predetermined service and generating a one time password when the IC card is input for the first time, and generating a one time password when the IC card is input at later times, and receiving a one time password generated in the terminal through a predetermined communication medium, and verifying the one time password. The initializing step of a service during the password generating step comprises the steps of reading the random number of the IC card and storing

it in the terminal, and deleting the random number from the IC card. The generating step of a one time password during the step of generating a password comprises the steps of reading the secret key of the IC card and the random number stored in the terminal, executing a symmetrical key cipher algorithm using the secret key and random number as an input, performing a one way hash function on the value output from the symmetrical key cipher algorithm, changing the random number into a predetermined value and storing it in the terminal, and converting the output of the one way hash function into a predetermined format. The verifying step comprises the steps of receiving the one time password generated in the terminal, through a predetermined communication medium, reading the secret key and the random number stored in the server, performing a symmetrical key cipher algorithm using the secret key and the random number as an input, performing a one way hash function on the value output from the symmetrical key cipher algorithm, changing the random number into a predetermined value and storing it in the terminal, and converting the output of the one way hash function into a predetermined format, and authenticating a user, if the predetermined format is the same as the received one time password, and not authenticating the user if not the same.

When the IC card comprises a private area and a public area of a memory and further comprises a card access key required for access to a secret area, initializing a service during the password generating step

comprises the steps of reading the random number and a card access key, for allowing access to the random number and private area, from the public area of the IC card and storing it in the terminal, and deleting the random number and the card access key from the public area of the IC card. The step of reading the secret key of the IC card during the password generating step comprises the steps of inputting the card access key stored in the terminal to the IC card, checking whether the card access key input to the IC card is the same as the card access key of the IC card private area, and if they are the same, allowing access to the card, and reading the secret key of the IC card when the access is allowed during the step of checking the card access key.

When the terminal and the server further comprise each counter for synchronizing the terminal with the server, the step of generating a one time password during the step of generating a password comprises the step of changing the random number and the counter value into predetermined values and storing them in the terminal. The step of generating a one time password during the step of generating a password comprises the steps of inserting the counter value into a password bit stream produced by the step of performing a one way hash function on the value output through the symmetrical key cipher algorithm, and converting the password bit stream into which the counter value is inserted into a predetermined format. The receiving step of the verifying step further comprises the steps of extracting a counter value from the received one time password, comparing the counter value extracted in the

extracting step with the counter value of the server, and making the counter values of the counter equal and changing the random number into a random number corresponding to the counter value, in the case that, in the comparing step, the counter values were not equal. The step of changing the random number of the verifying step is for changing the random number into a predetermined value and storing it in the terminal. The converting step of the verifying step comprises the steps of performing the one way hash function and inserting the counter value into the output password bit stream, and converting the password value into which the counter value is inserted into a predetermined format.

Brief Description of the Drawings

The above objective and advantages of the present invention will become more apparent by describing in detail a preferred embodiment thereof with reference to the attached drawings in which:

FIG. 1 is a block diagram of the structure of an apparatus for authenticating a user according to the present invention;

FIG. 2 is a block diagram of the detailed structure of a first password generator;

FIG. 3 is a block diagram of the detailed structure of a second password generator;

FIG. 4 is a flow chart of the overall operation of the apparatus for authenticating a user according to the present invention;

FIG. 5 is a flow chart of a service initializing process;

FIG. 6 is a flow chart of the detailed process of the step of generating a one time password of FIG. 4; and

FIG. 7 is a flow chart of a process of verifying the password transmitted by a user to the server of a service provider.

Detailed Description of the Invention

Hereinafter, the present invention will be described in detail with reference to the attached drawings. Referring to FIG. 1, an apparatus for authenticating a user according to the present invention includes an IC card 100 for safely keeping and carrying personal secret information, a terminal 120 which is subminiature so as to be easily carried, for generating a one time password for confirming the identity of a person and referring to an account balance of an electronic money, and a server 140 for authenticating the one time password generated in the terminal 120 and providing a service.

The IC card 100 stores a secret key and a predetermined random number for generating a one time password. The IC card 100 includes a public area 106 to which external access is allowed, a private area 108 for which a card access key is required in order to allow external access, a card access key memory 102 for storing the card access key required for accessing

the private area 108, and a card access checker 104 for comparing the card access key input from the outside with the card access key stored in the card access key memory 102 (set as a private area) and for determining whether access to inner information is allowed. The IC card 100 can be used as an identity card or to store electronic money and can keep plenty of information which a user cannot remember, since the memory capacity of the IC card 100 is much larger than that of a conventional magnetic card. Also, since the card access key of the IC card 100 is needed in order to read the data stored in the IC card, others cannot easily obtain the personal information of a user even if the user misplaces the IC card.

The terminal 120 is for receiving the IC card 100 and generating a one time password. The terminal 120 includes a card receiver 121, a random number memory 122, a first password generator 123, a first random number changer 124, a display 125, an inquiring portion 126, a counter memory 127, and a counter changer 128.

The card receiver 121 has a slot for receiving the IC card 100, and interfaces with the IC card 100. The random number memory 122 reads the random number stored in the IC card 100 when the IC card 100 is initially input to the card receiver 121, stores the random number, and deletes the random number stored in the IC card.

The first password generator 123 is for reading the secret key of the IC card 100 and the random number stored in the random number storing portion

122, and generating the one time password by a predetermined method. As shown in FIG. 2, the first password generator 123 includes a symmetrical key cipher portion 200, a hash function portion 210, and a first format converting portion 220. The symmetrical key cipher portion 200 reads the secret key of the IC card 100 and the random number of the random number memory 122, and generates a cipher using a symmetrical key cipher algorithm. The hash function portion 210 prevents an unauthorized person from inversely tracing the secret key and the random number, by converting the cipher generated in the symmetrical key cipher portion 200 using a one way hash function. The first format converting portion 220 is for converting the password bit stream output from the hash function portion 210 into a predetermined format which can be easily read by the user. The first format converting portion 220 includes a counter inserter 222, for inserting the counter value of the counter memory 127 into the password bit stream, and a format converter 224 for converting the password bit stream output from the counter inserter 222 into a predetermined format which can be easily read by the user. A protocol type selection (PTS) bit, which refers to the protocol of an algorithm for generating more than one one time password, can be additionally inserted by the counter inserter 222. The format converter 224 preferably converts a binary password bit stream into a decimal number which can be easily read by the user.

The first random number changer 124 changes the random number stored in the random number memory 122 into a predetermined value and

stores the changed random number in the random number memory 122 after the one time password is generated by the first password generator 123. The display 125 is for displaying the password generated in the first password generator 123. An LCD is preferably used as the display 125.

The inquiring portion 126 refers to the account balance and transaction records of the IC card 100. The counter memory 127 stores a counter value for synchronizing the terminal 120 with the server 140. The counter changer 128 changes the counter value into a predetermined value whenever one one time password is generated, and stores the value in the counter memory 127.

The server 140 is for authenticating a one time password generated in the terminal 120. The server 140 includes a secret key memory 141, a second password generator 144, a second random number changer 143, a password receiver 142, a password verifier 147, a counter memory 145, a counter changer 146, a counter extractor 148, and a random number synchronizer 149.

The secret key memory 141 stores a secret key and a random number, which are identical to the secret key initially stored in the IC card 100 and a predetermined random number, respectively.

The second password generator 144 is for reading the secret key and the random number stored in the secret key memory 141, and generating the one time password by the same method as a predetermined method used in the terminal 120. As shown in FIG. 3, the second password generator 144 includes a symmetrical key cipher portion 300, a hash function portion 310,

and a second format converting portion 320. The symmetrial key cipher portion 300 reads the secret key and the random number stored in the secret key memory 141, and generates a cipher using a symmetrical key cipher algorithm. The hash function portion 310 prevents an unauthorized person from inversely tracing the secret key and the random number, by converting the cipher generated in the symmetrical key cipher portion 300 using a one way hash function. The second format converting portion 320 is for converting the password bit stream output from the hash function portion 310 into a predetermined format. The second format converting portion 320 includes a counter inserter 322, for inserting the counter value of the counter memory 145 into the password bit stream, and a format converter 324 for converting the password bit stream output from the counter inserter 322 into a predetermined format which can be easily read by the user. The format converter 324 preferably converts the binary password bit stream into a decimal number which can be easily read by the user.

The second random number changer 143 makes the random number value of the secret key memory 141 identical to that of the first random number changer 124 of the terminal 120, and stores the changed value in the secret key memory 141 after the single-word password is generated by the second password generator 144. The password receiver 142 receives the one time password as displayed on the display 125 of the terminal 120 through a telephone line or a predetermined network.

The password verifier 147 checks whether the received password is identical to the generated password, and verifies the one time password. The counter memory 145 stores a counter value for synchronizing the terminal 120 with the server 140. The counter changer 146 changes the counter value into a predetermined value and stores it in the counter memory 145 whenever one one time password is generated.

The counter extractor 148 extracts the counter value from the one time password received by the password receiver 142, and extracts the PTS when the PTS is inserted by the counter inserter 222 of the terminal 120. The random number synchronizer 149 checks whether the counter value extracted by the counter extractor 148 coincides with the counter value of the server 140. If not, the random number synchronizer 149 generates a random number corresponding to the extracted counter value and inputs the random number to the symmetrical key cipher portion 300 of the server 140.

The operation of the apparatus for authenticating a user, and a method therefor, according to the present invention will be described as follows. In the present invention, a one time password which is changed each time the user is authenticated is used. A secret key, a random number, and a counter are used as variables for generating the one time password. The secret key for a symmetrical key cipher algorithm is used as a secret value for ciphering and is stored in the IC card 100 of each user. The random number for generating a different password every time exists in the IC card 100, is transmitted to and

stored in the portable terminal 120 in a process for initializing the service, and is deleted from the IC card. The counter for synchronizing the terminal 120 with the server 140 is kept in the terminal 120. The one time password is generated using the random number and the counter stored in the terminal 120. When the user wishes to be authenticated by various servers, IC cards for each service, but only one terminal, are necessary.

It is possible to synchronize the terminal 120 with the server 140 by including the counter value in the password during a process for generating the one time password. The server 140 extracts the counter value from the password received from the user, synchronizes with the terminal, generates the password using the secret key and the random number value shared with the terminal, and checks whether the generated password coincides with the password received from the user. It is possible to easily synchronize the terminal with the server even though only the counter of the terminal is changed, and the counter of the server is not changed so that the user accidentally changes the counter value. Also, the IC card 100 can request that the card access key be submitted in order to read information stored in the private area 108 in the card. It is possible to safely keep the private information of the user since only an authorized user can read the private information in the card by providing the card access key.

The operation of the present invention will be described in more detail. The user authentication apparatus according to the present invention has

functions of inquiring the account balance and trade details, initializing the service for generating a one time password, generating the one time password, and verifying the one time password in the server.

In the present invention, according to FIG. 4, the authentication of a user is performed using the one time password in three steps: initializing the service when a user inserts the IC card into the terminal in order to obtain the service (step 470), generating the one time password in the terminal (step 430), and verifying the password of the user in the server (step 450).

The user inserts the IC card 100 for the service which he or she wants into the card receiver 121 of the terminal 120 (step 400). When the user inserts the IC card, the card receiver 121 of the terminal 120 determines the kind of the IC card, and checks whether the IC card 100 is inserted for the first time, or was once inserted and initialized in the past (step 410). In the case of the IC card inserted for the first time, the initializing process (step 470) is performed. When the previously initialized IC card is inserted, it is determined whether the one time password is to be generated (step 420). Usually, the process is terminated after only the account balance is inquired (step 460). A user who wishes to be authenticated generates the one time password using the operating apparatus of the terminal (step 430). The terminal 120 submits the card access key received during the initializing process to the IC card 100, reads the secret values (a secret key for a symmetrical cipher algorithm) in the card, and generates the one time

password (step 430). When the user transfers this result to the server 140 (step 440), the server 140 verifies it (step 450).

FIG. 5 shows the service initializing process (step 470) in more detail. The service initializing process (step 470) is for transmitting the card access key, for reading the random number which is critical to the user authentication stored in the public area of the IC card and the secret key stored in the private area of the IC card of the user, to the terminal and for deleting the random number and the card access key from the public area, after the user inserts the IC card 100 into the terminal 120 for the first time (the step 400 of FIG. 4). At this time, the terminal 140 senses that the IC card 100 is inserted for the first time, and performs the initializing process. The terminal 140 reads the random number and the card access key stored in the public area of the IC card 100 (step 510), stores them in the random number memory 122 of the terminal 140 (step 520), and deletes the random number and the card access key from the public area of the IC card 100 (step 530). Therefore, only the secret key remains in the safe private area of the initialized IC card.

The information of the IC card for referring to the account balance is open to everyone. The card access key is required for reading the secret key for the user authentication, stored in the secret area. After the service initializing process is performed, the secret key in the IC card can be read by only the terminal which performed the initializing process. The user can generate a one time password for various services with one terminal. Separate

memory spaces are assigned in the terminal to the respective services. Information required for authenticating the user of the respective services is kept in the memory spaces.

FIG. 6 is a flow chart showing the operation in the step 430 of generating the one time password of FIG. 4 in more detail. The one time password is generated using the secret key (secret keys for the symmetrical key cipher algorithm), shared by the IC card 100 and the server 140, and a random number value shared by the terminal 120 and the server 140. When the user inserts the IC card into the terminal (step 400 of FIG. 4) and commands the terminal to generate a one time password, the symmetrical key cipher portion 200 of the first password generator 123 in the terminal 120 reads the secret key from the IC card 100 and the random number and the counter value from the random number memory 122 (step 610), generates a cipher from the read values using the symmetrical key cipher algorithm (step 620), and calculates the resultant binary value using a one way hash function in the hash function portion 210 (step 630). The one way hash function is used in order to prevent a person attempting unauthorised access from finding out any information on the secret value using the result of the one time password.

The resultant value of the one way hash function undergoes a conversion algorithm process since it cannot be directly used as a one time password (step 680). First, the binary resultant value which would be

unfamiliar to the user is changed into a decimal number which can be easily used by the user. The one time password, converted to decimal form, is displayed on the display 125 (step 690). Since the binary number output by the one way hash function is very big (for example, a binary number of more than 64 bits), it must be changed into a number within a certain size (for example, a binary number of about 26 bits in the case of using a decimal number of eight figures as the one time password) which can be displayed on the display 125 of the terminal.

In the conversion algorithm (step 680), the resultant value of the one way hash function, the counter value, and the protocol type selection (PTS) are used. Here, the PTS and the counter value N are inserted into the bit stream of the one time password by the counter inserter 222, in order to synchronize the terminal 120 with the server 140. For example, the password of 26 bits is divided into an area occupied by the resultant value of the one way hash function and an area occupied by the counter value N and the PTS. The PTS is required when the server categorizes various algorithms for generating the one time password.

The counter value N is reduced by one each time a password is generated (step 650). It is checked whether the reduced value is 0 (step 640). When the value becomes 0, the process returns to an initial stage. The random number is usually increased by one and initialized when N becomes 0. In the process of initializing the service, the random number read and used in

the IC card is used only for generating the initial password and, after the initial one, the random number is increased by one when each password is generated (step 650). When the counter value N becomes 0, a random number generated during the generation of the password (for example, the resultant value of the symmetrical key cipher algorithm) is set as the random number initialized value. The password is generated by increasing the random number by one (step 650). A new random number is set when the counter value N becomes 0 (step 660). After generating a password, the counter value N and the random number RN are recorded in the random number memory 122 (step 670).

FIG. 7 is a flow chart of a process for verifying the password transferred by the user to the server 140 of the service provider. The server 140 receives the one time password transferred by the user through the password receiver 142 (step 700). Then, the server extracts the counter value from the data bit stream received by the counter extracter 148 (step 710) and synchronizes with the terminal 120. The server 140 generates a one time password by the same method as in the terminal, using the synchronized random number and secret number (step 720). Since the process for generating the one time password is the same as that in the terminal, an explanation thereof is omitted. Then, the generated one time password is compared with the one generated by the user (step 730). If the two passwords are identical, the identity of the user is authenticated (step 770).

If the password transferred by the user does not coincide with the one generated in the server 140, it means that an unauthorized person attempts to use the card, or that the terminal 120 of the user is not synchronized with the server 140. In the case that the one time password transferred by the authorized user does not coincide with the password generated in the server 140, it means that the user made a mistake or the counter value of the terminal 120 does not coincide with that of the server 140. Namely, even though the counter value of the terminal 120 is the same as that of the server 140, the passwords may not be the same due to the difference in the random number value, when the periods N of the two counters are different. The server 140 increases the counter value and the random number, calculates the password, and compares the password with the password transferred by the user in units of the period of the counter in order to compensate for this. It is not necessary for the server 140 to calculate all the passwords of N times in order to calculate the passwords after the period N times. Since only an additional calculation for setting a new random number is necessary when the N becomes 0, a great amount of calculating is not necessary (step 760). In the case that the passwords after the Nth password do not coincide with the password transferred by the user, the passwords after the Nth password must be calculated again. It is possible to determine how many times such a process should be repeated, if necessary (step 740). If the password transferred by the user does not coincide with the password of the server

within a designated time, it is determined to be an attempt by an unauthorized person and the service is rejected (step 750).

As mentioned above, it is possible to improve the security level by additionally using the password remembered by the user for the user authentication in which only the IC card 100 and the portable terminal 120 of the user are used. If the user misplaces the IC card 100 and the terminal 120, a person who knows the personal information on the user may be authenticated by obtaining them. If the process for confirming the password remembered by only the user is added to the user authentication process of the present authentication system, a safer user authentication is available. Namely, the user should own the password remembered by only the user, the IC card owned by only the user, and the portable terminal for generating the one time password in order to be authenticated as the authorized user.

As mentioned above, the user uses the terminal in order to generate the one time password. A unique secret key for generating a different one time password to every user exists in the terminal. The secret key should be included in the server in order to verify the one time password transferred by the user. Here, the secret key may be inserted into the terminal in the factory during manufacture. However, the secret key is preferably inserted into the terminal when a service provider performs a user registration of the terminal. The service provider generates a secret key for the terminal, inserts it into the terminal through the IC card, and registers it on the server.

By doing so, an additional process is not required for inserting the secret key when the terminal is manufactured. Accordingly, it is possible to improve productivity when the terminal is mass-produced in the factory. Also, the secret key for the user authentication, which is known to only the service provider, is safe and in no danger of being exposed. Here, the terminal producer or the service provider do not have to preconfigure the terminal before it is provided to a user.

In the present invention, the security level is heightened by using a one time password in which the password changes each time a user is authenticated.

In the present invention, the security level is much higher than in a conventional user authentication method, since a correct one time password is generated only when the IC card 100 owned by the user coincides with the terminal 120 owned by the user, thus an unauthorized person cannot generate a correct password even if he or she obtains the terminal or the IC card of an authorized user. Also, the password, the IC card, and the terminal for generating the password of the user are essential to authentication as an authorized user, since a process for confirming the password remembered only by the user is added during the process for authenticating the user.

In the present invention, the exposure of the private information is prevented and the one time password for various services is generated by one terminal, since the user uses the IC card and the portable terminal of his or her

own in order to generate the one time password, and sets a card access key for reading the information in the IC card for storing the private information of the user.

The present invention is easily implemented as software in a conventional system for authenticating the user, using the random number in order to generate the one time password and the counter in order to synchronize the terminal of the user with the server of the service provider. Accordingly, it is possible to cost-efficiently enhance the user authentication without additional cost to the service provider.

The apparatus for authenticating the user and the method therefor in the present invention can be applied everywhere a user authentication is required, such as telebanking, home shopping and banking using a PC, a paid PC communication, and a network service. Especially, the user need not directly go to the service provider for a service registration. The user applies for a service, receives an IC card by mail from a service provider, obtains a terminal from a shop, and is safely authenticated. This is very convenient in a situation in which it is difficult for the user to visit the service provider. Also, the service provider does not have to face users for mass delivered services.

The terminal used in the present invention can generate the one time password and refers to the account balance and transaction records of the electronic money of a general IC card. The terminal of the present invention

is very useful considering that the usage of electronic money will rapidly spread.

CLAIMS:

1. An apparatus for authenticating a user, comprising:

an integrated circuit (IC) card for storing a secret key for generating a one time password and predetermined random numbers;

a terminal for generating a one time password using said IC card as an input; and

a server for authenticating the one time password generated by said terminal,

wherein said terminal comprises:

a card receiver for receiving and interfacing with said IC card, and determining whether said IC card is input for the first time;

a random number memory for reading and storing, and then deleting the random numbers of said IC card when said IC card is inserted for the first time into said card receiver;

a first password generator for generating a one time password by reading the secret key of said IC card and the random number stored in said random number memory;

a first random number changer for changing the random number stored in said random number memory into a predetermined value and storing the changed value in said random number memory when a one time password is generated in said first password generator; and

a display for displaying the processed results of said terminal and said server, and

wherein said server comprises:

a secret key memory for storing a secret key and a predetermined random number identical to the secret key and a predetermined random number initially stored in said IC card;

a second password generator for reading the secret key and the random number stored in said secret key memory and for generating a one time password by the same method as used in the terminal;

a second random number changer for changing the random number value of said secret key memory into a value identical to the random number changer of said terminal, and storing the changed value in the secret key memory when a one time password is generated by said second password generator;

a password receiver for receiving the one time password generated in said terminal through a telephone line or a network; and

a password verifier for verifying whether said received password is identical to said generated password.

2. An apparatus for authenticating a user as claimed in claim 1, wherein said IC card is used both as an identity card and for electronic money, and safely stores a secret value for authenticating a user.

3. An apparatus for authenticating a user as claimed in claim 1, wherein the secret key of said terminal is initially inserted into said terminal by a service provider during a user registration process.

4. An apparatus for authenticating a user as claimed in claim 1, wherein said IC card further comprises:

a card access key memory comprising a public area, to which access is allowed unconditionally, and a private area for which a card access key is required to allow access from the outside for safely storing a card access key required for allowing access to said secret area; and

a card access checker for determining whether access to internal information should be allowed, by comparing said card access key input from the outside with the card access key stored in said card access key memory, and

wherein the random number memory of said terminal reads the random number and card access key of said IC card and stores them, and deletes the random number and card access key from the public area of said IC card, when said IC card is inserted into said card receiver for the first time.

5. An apparatus for authenticating a user as claimed in claim 1, wherein said terminal further comprises an inquiring portion for inquiring the account balances and transaction records of said IC card.

6. An apparatus for authenticating a user as claimed in claim 4, wherein the first password generating portion of said terminal comprises:

a symmetrical key cipher portion for reading the secret key of said IC card and the random number of said random number memory and generating a cipher using a symmetrical key cipher algorithm;

a hash function portion for converting the cipher generated in said symmetrical key cipher portion, using a one way hash function, to prevent an inverse trace of said secret key; and

a format converter for converting the cipher output from said hash function portion into a predetermined format, and wherein the second password generating portion of said server comprises:

a symmetrical key cipher portion for reading the secret key and the random number stored in said secret key storing portion and for generating a cipher using a symmetrical key cipher algorithm;

a hash function portion for preventing an inverse trace of the cipher generated in said symmetrical key cipher portion, using a one way hash function; and

a format converter for converting the cipher output from said hash function portion into a predetermined format.

7. An apparatus for authenticating a user as claimed in claim 6, wherein said terminal and server further comprise:

a counter memory for storing a counter value for synchronizing said terminal with said server; and

a counter changer for changing said counter value into a predetermined value, whenever a one time password is generated, and storing the new value in said counter memory,

wherein the format converter of said first password generater and the format converter of said second password generator each further comprise a counter inserter for inserting the counter value of said counter memory into a password bit stream output from said hash function portion, and

wherein said server further comprises:

a counter extractor for extracting a counter value from the one time password received by said password receiver; and

a random number synchronizer for generating a random number corresponding to said extracted counter value and inputting it to the symmetrical key cipher portion of said server, in the case that the counter value extracted by said counter extractor does not coincide with the counter value of said server.

8. An apparatus for authenticating a user as claimed in claim 7, wherein said format converter converts a binary number into a decimal number.

9. An apparatus for authenticating a user as claimed in claim 7, wherein each of the counter inserters of said terminal and said server additionally inserts a PTS bit which refers to the protocol of an algorithm for generating more than one one time password, the counter extractor of said server further extracts said PTS bit, and the first and second password generators generate a one time password using an algorithm for generating a one time password according to the information of said PTS.

10. A method for authenticating a user, using a user authenticating apparatus comprising an IC card for storing a predetermined random number and a secret key for generating a one time password, a terminal for generating a one time password using said IC card as an input, and a server for storing the secret key and a random number identical to those of said IC card and for authenticating the one time password generated in said terminal, the user authenticating method comprising the steps of:

inserting said IC card into said terminal;

determining whether said IC card is input to said terminal for the first time;

initializing a predetermined service and generating a one time password when said IC card is input for the first time, and generating a one time password when said IC card is input at later times; and

receiving a one time password generated in said terminal through a predetermined communication medium, and verifying said one time password,

wherein said initializing step of a service during said password generating step comprises the steps of:

reading the random number of said IC card and storing it in the terminal; and

deleting the random number from said IC card,

wherein said generating step of a one time password during said step of generating a password comprises the steps of:

(a) reading the secret key of said IC card and the random number stored in said terminal;

(b) executing a symmetrical key cipher algorithm using said secret key and random number as an input;

(c) performing a one way hash function on the value output from said symmetrical key cipher algorithm;

(d) changing said random number into a predetermined value and storing it in the terminal; and

(e) converting the output of said one way hash function into a predetermined format; and

wherein said verifying step comprises the steps of:

receiving the one time password generated in said terminal, through a predetermined communication medium;

reading the secret key and the random number stored in said server;

performing a symmetrical key cipher algorithm using said secret key and said random number as an input;

performing a one way hash function on the value output from said symmetrical key cipher algorithm;

changing said random number into a predetermined value and storing it in the terminal; and

converting the output of said one way hash function into a predetermined format; and

authenticating a user, if said predetermined format is the same as said received one time password, and not authenticating the user if not the same.

11. A method for authenticating a user as claimed in claim 10, when said IC card further comprises a card access key required for access to a

secret area, wherein initializing a service during said password generating step comprises the steps of:

reading the random number and a card access key, for allowing access to the random number and private area, from the public area of said IC card and storing it in the terminal; and

deleting the random number and the card access key from the public area of said IC card, and

wherein said step (a) of reading the secret key of the IC card during said password generating step comprises the steps of:

inputting the card access key stored in said terminal to said IC card;

checking whether the card access key input to said IC card is the same as the card access key of said IC card private area, and if they are the same, allowing access to the card; and

reading the secret key of said IC card when the access is allowed during said step of checking the card access key.

12. A method for authenticating a user as claimed in claim 11, when said terminal and said server further comprise each counter for synchronizing the terminal with the server wherein said step (d) of generating a one time password during said step of generating a password comprises the step of changing said random number and said counter value into predetermined values and storing them in the terminal,

wherein said step (e) of generating a one time password during said step of generating a password comprises the steps of:

inserting said counter value into a password bit stream produced by said step (c) of performing a one way hash function on the value output through said symmetrical key cipher algorithm; and

converting the password bit stream into which said counter value is inserted into a predetermined format,

wherein said receiving step of said verifying step further comprises the steps of:

extracting a counter value from the received one time password;

comparing the counter value extracted in said extracting step with the counter value of said server; and

making the counter values of said counter equal and changing said random number into a random number corresponding to said counter value, in the case that, in said comparing step, the counter values were not equal,

wherein said step of changing said random number of said verifying step is for changing said random number into a predetermined value and storing it in the terminal, and

the converting step of said verifying step comprises the steps of:

performing said one way hash function and inserting said counter value into the output password bit stream; and

converting the password value into which said counter value is inserted into a predetermined format.

13. An apparatus for authenticating a user, comprising:

an integrated circuit (IC) card for storing a secret key for generating a single-use password and a predetermined random number;

a terminal for generating a single-use password using said IC card as an input; and

a server for authenticating the single-use password generated by said terminal,

wherein said terminal comprises:

an interface for interfacing with said IC card;

a random number memory for storing the random number held in said IC card;

a first password generator for generating a single-use password by reading the secret key of said IC card and the random number stored in said random number memory;

a means for changing the random number stored in said random number memory to a predetermined value when a single-use password is generated in said first password generator; and

wherein said server comprises:

a means for storing a secret key and a predetermined random number identical to the secret key and a predetermined random number initially stored in said IC card;

a second password generator for reading the secret key and the random number stored in said storing means for generating a single-use password by the same method as used in the terminal;

a means for changing the random number stored in said storing means to the value of the changed random number stored in the random number memory of said terminal, when a single-use password is generated by said second password generator;

a password receiver for receiving the single-use password generated in said terminal; and

a password verifier for verifying whether said received password is identical to said generated password.

14. A user authentication apparatus substantially as herein described with reference to the accompany drawings.

15. A user authentication method substantially as herein described with reference to the accompany drawings.

Patent Office

41

Application No: GB 9721224.5
Claims searched: 1-15

Examiner: Mike Davis
Date of search: 23 January 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4H (HTG), H4P (PDCSA)

Int Cl (Ed.6): G07F, H04L, G06F

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
	None	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.